Amendment to the Claims

This listing of the claims replaces all prior versions and listings of claims in the application. Please amend claims 1, 3, 5, 7, 9-20, 22-23 and add new claims 24-27 as follows:

Claim 1 (Currently amended). A method for enabling a client terminal to access a wireless network, comprising:

receiving an access request from the client terminal;

redirecting the access request to a local web server via a packet traffic filter for filtering packet traffic;

requesting from the client terminal, information required to establish client terminal access to the wireless network;

activating, in response to the information received from the client terminal, a ~~software~~ module that reconfigures the client terminal for authentication using appropriate parameters associated with a configuration arrangement selected by a user; and

authenticating the reconfigured client terminal and allowing access to the wireless network in response to the authentication.

Claim 2 (Previously presented). The method according to claim 1, wherein the wireless network is an IEEE 802.11 compliant wireless local area network (WLAN), and the client terminal is an IEEE 802.1x compliant client terminal.

Claim 3 (Currently amended). The method according to claim 2, wherein the activating step comprises activating an Active X control/plug-in ~~previously~~ installed on the client terminal.

Claim 4 (Original). The method according to claim 2, wherein the activating step comprises downloading to, and activating in, the client terminal an Active X control/plug-in.

Claim 5 (Currently amended). An access point for providing a secure communications session between a client terminal and a wireless network, comprising:

a means for receiving an access request from the client terminal;

means for redirecting the access request to a local web server for allowing a reconfigured access to the wireless network via a packet filter means for filtering packet traffic,

means for activating, in response to the information received form the client terminal, a software module that reconfigures the client terminal for authentication using appropriate parameters associated with a configuration arrangement selected by a user; and

means for authenticating the reconfigured client terminal and allowing access to the wireless network in response to the authentication.

Claim 6 (Original). The access point according to claim 5, wherein the access point complies with the IEEE 802.11 standards and the client terminal is an IEEE 802.1x compliant client terminal.

Claim 7 (Currently amended). A method for configuring a client terminal to provide secure access in a wireless network, comprising:

filtering traffic associated with ~~an HTTP~~ a first request from the client terminal for access to the wireless network, at a packet traffic filter for filtering packet traffic;

redirecting the access request to a designated web server, via said packet traffic filter for filtering packet traffic; and

issuing a second request from the designated web server to the client terminal for information required to establish an authorized communication.

Claim 8 (Previously presented). The method according to claim 7, wherein the wireless network is an IEEE 802.11 compliant wireless local area network and the client terminal is an IEEE 802.1x compliant client terminal.

Claim 9 (Currently amended). The method according to claim ~~8~~ 7, further comprising ~~the step of~~ receiving from the client terminal ~~providing the web server~~ and communicating to the designated web server information required to establish an authorized connection.

Claim 10 (Currently amended). The method according to claim ~~8~~ 7, further comprising ~~the step of~~ receiving from the designated web server and communicating to the client terminal access

rate information required to establish an authorized communication.

Claim 11 (Currently amended). The method according to claim ~~8~~, further comprising ~~the step of~~ receiving from the designated web server and communicating to the client terminal access user account creation information required to establish an authorized communication.

Claim 12 (Currently amended). The method according to claim ~~8~~ 7, further comprising ~~the step of~~ receiving from the designated web server and communicating to the client terminal access authentication method selection information required to establish an authorized communication.

Claim 13 (Currently amended). The method according to claim ~~8~~ 7, further comprising ~~the step of~~ receiving from the designated web server and communicating to the client terminal new account creation information required to establish an authorized communication.

Claim 14 (Currently amended). The method according to claim ~~8~~ 7, further comprising ~~the step of~~ receiving from the designated web server and communicating to the client terminal access user terms and conditions of acceptance information required to establish an authorized communication.

Claim 15 (Currently amended). The method according to claim ~~8~~ 7, further comprising ~~the step of~~ receiving from the client terminal and communicating to the designated web server access rate information required to establish an authorized communication.

Claim 16 (Currently amended). The method according to claim ~~8~~ 7, further comprising ~~the step of~~ receiving from the client terminal and communicating to the designated web server user account creation data required to establish an authorized communication.

Claim 17 (Currently amended). The method according to claim ~~8~~ 7, further comprising ~~the step of~~ receiving from the client terminal and communicating to the designated web server user access authentication method selection information required to establish an authorized communication.

Claim 18 (Currently amended). The method according to claim ~~8~~ 7, further comprising ~~the step of~~ receiving from the client terminal and communicating to the designated web server acceptance of the user access terms and conditions required to establish an authorized communication.

Claim 19 (Currently amended). The method according to claim 8, whereby authorization is browser based and the browser program is an ActiveX control.

Claim 20 (Currently amended). The method according to claim 8, whereby authorization is browser based and the browser program is a plug-in.

Claim 21 (Previously presented). A mobile terminal, comprising:

means for receiving an extended authentication protocol request identification message packet;

means for forwarding an extended authentication protocol response identity message packet;

means for receiving an extended authentication protocol failure message packet;

means for forwarding a web re-direct request via a packet traffic filter for filtering packet traffic;

means for receiving a provider list web page;

means for selecting a provider and forwarding said selected provider information;

means for receiving an ActiveX control message to re-configure said mobile terminal; and

means for reconfiguring said mobile terminal and establishing authorized communications.

Claim 22 (Currently amended). The~~A~~ method as recited in claim 1, the method further comprising

creating a plurality of operating states, said packet traffic filter receiving wireless local area network state information from said access point.

Claim 23 (Currently amended). The~~A~~n access point as recited in claim 5, the access point creating a plurality of operating states wherein said packet traffic filter means receives wireless local area network state information from said access point.

Claim 24 (New). An access point associated with a communications network, comprising:

means for forwarding an extended authentication protocol request identification message packet;

means for receiving an extended authentication protocol response identity message packet;

means for forwarding an extended authentication protocol failure message packet to a client terminal responsive to a state failure;

means for receiving a re-direct client request from said forwarding means at a packet filter module responsive to said state failure;

alternative means for receiving a request for access to a communications network at said packet filter module responsive to said state failure; and

means for forwarding a web re-direct request via said packet filter module and for establishing authorized communications following successful reconfiguration responsive to authentication.

Claim 25 (New). The method according to claim 1, further comprising:

detecting a state failure; and

redirecting the access request to a local web server via said packet traffic filter responsive to one of the packet traffic filter receiving a redirect client request and of receiving a web access request from said client terminal after detection of said state failure.

Claim 26 (New). The access point according to claim five, further comprising:

an 802.1x engine for detecting a state failure; and

said packet traffic filter means redirecting the access request to a local web server responsive to one of the packet traffic filter means receiving a redirect client request from said

802.1x engine and of receiving a web access request from said client terminal after detection of said state failure.

Claim 27 (New). The method according to claim 7, further comprising:

detecting a state failure; and

redirecting the access request to said designated web server via said packet traffic filter responsive to one of the packet traffic filter receiving a redirect client request and of receiving a web access request from said client terminal after detection of said state failure.